CLAIMS

1. Computer apparatus comprising a processor arranged to generating a cryptographic key using a first data set that corresponds to a first identifier, a second data set that corresponds to a first trusted party's public key, a third data set that corresponds to a second identifier and a fourth data set corresponds to a second trusted party's public key.

2. Computer apparatus according to claim 1, wherein the first and third data sets are public parameters.

3. Computer apparatus according to claim 1, wherein the first and third data sets are private parameters respectively generated by the first and third trusted parties.

4. Computer apparatus according to claim 1, wherein the second and fourth data sets are public parameters.

5. Computer apparatus according to claim 2, wherein the second and fourth data sets are public parameters.

6. Computer apparatus according to claim 3, wherein the second and fourth data sets are public parameters.

7. Computer apparatus according to claim 1, wherein the first and second data sets comprise a first common parameter associated with said first identity and said first trusted party, and the third and fourth data sets comprise a second common parameter associated with said second identity and said second trusted party.

8. Computer apparatus according to claim 1, wherein the cryptographic key is an encryption key.

9. Computer apparatus according to claim 8, wherein the processor is arranged to encrypt a fifth data set with the encryption key.

10. Computer apparatus according to claim 9, wherein the processor is arranged to encrypt the fifth data set with the encryption key and a random number.

11. Computer apparatus according to 8, wherein the processor is arranged form said encryption key using a bilinear pairing operating on the first and second data sets and the third and fourth data sets.

12. Computer apparatus according to claim 11, wherein the bilinear pairing is either a Tate or Weil pairing.

13. Computer apparatus according to claim 1, wherein the cryptographic key is a decryption key.

14. Computer apparatus according to claim 13, wherein the processor is arranged to form the decryption key using a bilinear pairing operating on the first and second data sets and the third and fourth data sets.

15. Computer apparatus according to claim 14, wherein the bilinear pairing is either a Tate or Weil pairing.

16. Computer apparatus according to claim 1, wherein the cryptographic key is a signature key.

17. Computer apparatus according to claim 16, wherein the processor is arranged to sign a sixth data set with the signature key.

18. Computer apparatus according to claim 17, wherein the processor is arranged to sign the sixth data set with the signature key and a random number.

19. Computer apparatus according to claims 16, wherein the processor is arranged to form the signature key using a bilinear pairing operating on the first and second data sets and the third and fourth data sets.

20. Computer apparatus according to claim 19, wherein the bilinear pairing is either a Tate or Weil pairing.

21. Computer apparatus according to claim 1, wherein the cryptographic key is a verification key.

22. Computer apparatus according to claim 21, wherein the processor is arranged to verify a signed data set with the verification key.

23. Computer apparatus according to claim 21, wherein the processor is arranged to form the verification key using a bilinear pairing operating on the first and second data sets and the third and fourth data sets.

24. Computer apparatus according to claim 23, wherein the bilinear pairing is either a Tate or Weil pairing.

25. A method comprising generating a cryptographic key using a first data set that corresponds to a first identifier, a second data set corresponds to a first trusted party's public key, a third data set that corresponds to a second identifier and a fourth data set that corresponds to a second trusted party's public key.

26. A method according to claim 25, further comprising encrypting a fifth data set with the cryptographic key.

27. A method according to claim 25, wherein the encryption key is formed using a Tate or Weil pairing operating on the first and second data sets and the third and fourth data sets.

28. A computer system comprising a first computer entity arranged to generate a first data set that corresponds to a first trusted party's public key; a second computer entity arranged to generate a second data set that corresponds to a second trusted party's public key; and a third computer entity arranged to generate a cryptographic key using a first identifier in conjunction with the first data set and a second identifier in conjunction with the second data set.

29. A computer system according to claim 28, wherein the third computer entity is arranged to encrypt a third data set with the cryptographic key.

30. A computer system according to claim 29, wherein the third computer entity encrypts the third data set using a bilinear pairing when operating on the first and third data sets and the second and fourth data sets.

31. A computer system according to claim 30, wherein the bilinear pairing is either a Tate or Weil pairing.

32. A computer system according to claim 28, wherein the first data set and second data set are public data parameters.

33. A computer system according to claim 28, wherein the public data parameters include an elliptic curve and a generator point on the elliptic curve.

34. A method of generating a cryptographic key wherein a bilinear mapping function is used to process multiple data sets each comprising data related to a respective association of trusted authority and user identity.

35. A method according to claim 34, wherein the cryptographic key is an encryption key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on a secret of the latter.

36. A method according to claim 34, wherein the cryptographic key is a decryption key, each data set comprising an identity-based private key derived from said user identity and a secret of the trusted authority.

37. A method according to claim 34, wherein the cryptographic key is a signature key, each data set comprising an identity-based private key derived from said user identity and a secret of the trusted authority.

38. A method according to claim 34, wherein the cryptographic key is a verification key, each data set comprising an identity-based public key derived from said user identity, and a public key element of the trusted authority that is based on a secret of the latter.

39. A method according to claim 34, wherein at least two said data sets relate to different user identities and at least two said data sets relate to different trusted authorities.

40. A method according to claim 34, wherein at least two said data sets relate to different user identities.

41. A method according to claim 35, wherein at least two said data sets relate to different trusted authorities.

42. A method according to claim 41, wherein said different trusted authorities are associated with different elements to which said bilinear mapping function can be

applied, each trusted authority having an associated public key formed from its associated element and a secret of that trusted authority.

43. A computer program product arranged, when installed in computing apparatus, to condition the apparatus for generating a cryptographic key by using a bilinear mapping function to process multiple data sets each comprising data related to a respective association of trusted authority and user identity.

44. A method according to claim 35, wherein there are n data sets and the encryption key is generated as:

$$\prod_{1 \le i \le n} \hat{p}(R_{TAi}, r\, Q_{IDi})$$

where:

$\hat{p}()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the i^{th} data set,

R_{TAi} is the public key element of the trusted authority associated with the i^{th} data set, and

r is a random number.

45. A method according to claim 36, wherein there are n data sets and the decryption key is generated as:

$$\hat{p}(U, \sum_{1 \le i \le n} S_i)$$

where:

$\hat{p}()$ is said bilinear mapping function,

S_i is the identity-based private key associated with the i^{th} data set, and

U is an element based on a random number and an element of a public key of the trusted authority associated with the i^{th} data set.

46. A method according to claim 37, wherein there are n data sets and the signature key is generated as:

$\mathbb{p}(\Sigma_{(1 \le i \le n)} d_{IDi}, P)$

where:

$\mathbb{p}()$ is said bilinear mapping function,

d_{IDi} is the identity-based private key associated with the i^{th} data set, and

P is a public key element of the trusted authority associated with the i^{th} data set.

47. A method according to claim 38, wherein there are n data sets and the verification key is generated as:

$\Pi_{(1 \le i \le n)} \mathbb{p}(Q_{IDi}, P_{pubi})$

where:

$\mathbb{p}()$ is said bilinear mapping function,

Q_{IDi} is the identity-based public key associated with the i^{th} data set, and

P_{pubi} is the public key element of the trusted authority associated with the i^{th} data set.

48. A method according to claim 34, wherein:

- the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve;
- the point associated with the user identity is formed by a map-to-point hash function applied to the user identity, the combination of this point with a secret of the trusted authority forming an identity-based private key; and
- the point associated with the trusted authority forms, together with a combination of this point with a secret of the trusted authority, a public key of the trusted authority.

49. A method according to claim 34, wherein the bilinear mapping function pairing is one of a Tate pairing and a Weil pairing.